The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
12/21/2020

SUBJECT:
Multiple Vulnerabilities in Treck TCP/IP Stack Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Treck TCP/IP Stack, the most severe of which could result in arbitrary code execution. Treck TCP/IP Stack are networking protocols libraries specifically designed for embedded systems and are widely used. Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the application. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Treck TCP/IP stack Version 6.0.1.67 and prior

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Treck TCP/IP Stack, the most severe of which could result in arbitrary code execution. Details of these vulnerabilities are as follows:

- A heap-based buffer-overflow vulnerability. Specifically, this issue exists in Treck HTTP Server components. An unauthenticated attacker can exploit this issue to cause a denial-of-service conditions or to execute arbitrary code. [CVE-2020-25066]
- A denial-of-service vulnerability. Specifically, this issue occurs due to an out of bounds write error in the IPv6 component. [CVE-2020-27337]
- A denial-of-service vulnerability. Specifically, this issue occurs due to an out of bounds write error DHCPv6 client component. [CVE-2020-27338]
- An input-validation vulnerability. Specifically, this issue affects the IPv6 component. An attacker can exploit this issue to cause out of bounds read of up to three bytes. [CVE-2020-27336]

An attacker can exploit these issues to execute arbitrary code in the context of the user running the affected application and cause denial-of-service conditions.

RECOMMENDATIONS:
The following actions should be taken:

- Run all software as a nonprivileged user with minimal access rights. To reduce the impact of latent vulnerabilities, always run non-administrative software as an unprivileged user with minimal access rights.
- Deploy network intrusion detection systems to monitor network traffic for malicious activity.
- Deploy NIDS to monitor network traffic for signs of anomalous or suspicious activity. This includes but is not limited to requests that include NOP sleds and unexplained incoming and outgoing traffic. This may indicate exploit attempts or activity that results from successful exploits.
- Do not accept or execute files from untrusted or unknown sources.
- To reduce the likelihood of successful exploits, never handle files that originate from unfamiliar or untrusted sources.
- Implement multiple redundant layers of security. Since this issue may be leveraged to execute code, we recommend memory-protection schemes, such as nonexecutable stack/heap configurations and randomly mapped memory segments. This tactic may complicate exploits of memory-corruption vulnerabilities.

REFERENCES:
Treck:
https://treck.com/
https://treck.com/vulnerability-response-information/

CISA:
https://us-cert.cisa.gov/ics/advisories/icsa-20-353-01

CVE:
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2020-25066
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2020-27336
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2020-27337
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2020-27338